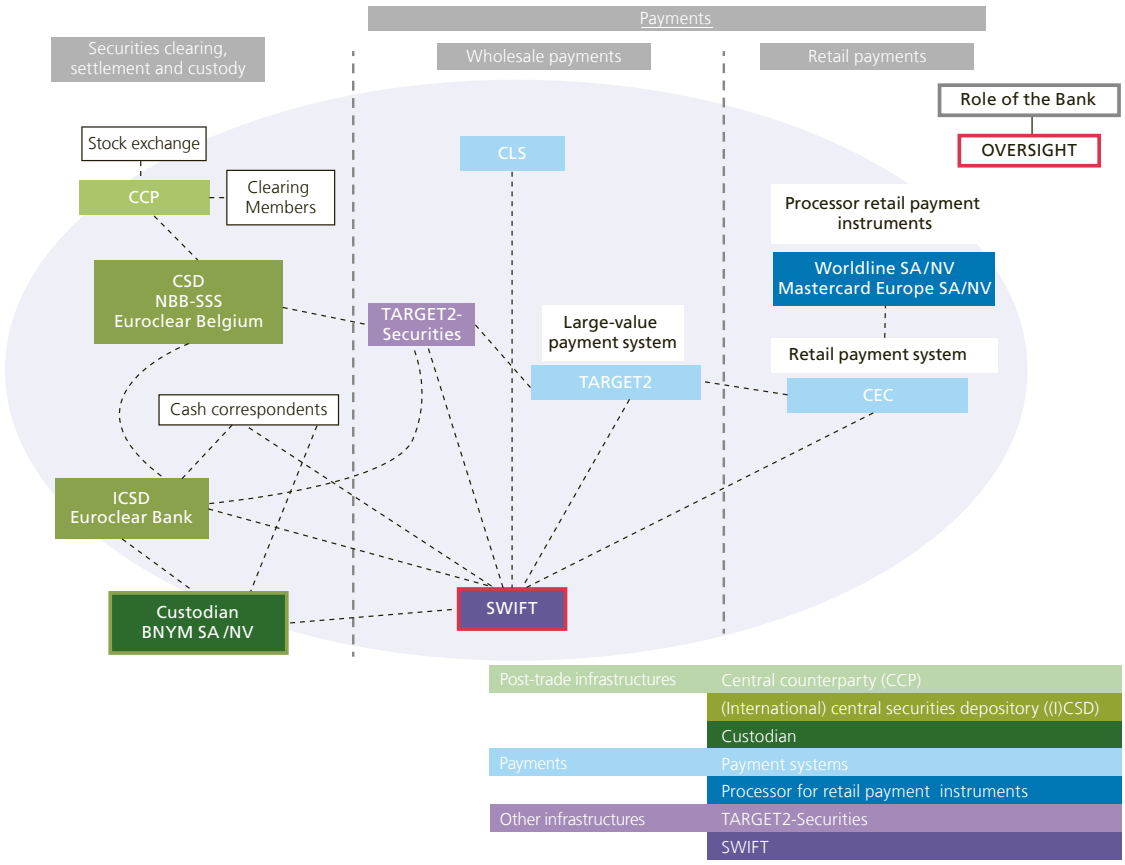
4. SWIFT

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a limited liability cooperative company registered in Belgium. SWIFT provides messaging and connectivity services to a wide variety of financial institutions and market infrastructures, including banks, brokers, investment managers, fund administrators, trading institutions, treasury counterparts and trusts.

SWIFT is a critical service provider to systemically important correspondent banking activities and financial market infrastructures (see chart 5). Therefore, the G10 central banks have identified SWIFT as systemically important.

Chart 5

SWIFT as a critical service provider to the financial industry



4.1 Oversight approach

An international cooperative arrangement has been established to oversee the safe and efficient functioning of SWIFT. As SWIFT is based in Belgium, the National Bank of Belgium has been appointed as lead overseer.

BOX 11

International dimension of SWIFT

SWIFT operates in an international context by having activities in more than 200 countries. In 2019, 8.4 billion FIN messages (+7.4 % compared to 2018) were sent, with a daily average of 33.5 million messages.

SWIFT's users own the company and interact with the Board and Executive Committee through national member groups[1], user groups[2] and dedicated workgroups. Shares are allocated based on message traffic over the SWIFT network. Every three years, there is a redistribution of the shares to realistically reflect changes in the use of SWIFT messaging. Countries or country constituencies appoint directors to the SWIFT Board based on the number of shares owned by all users in the country. The next redistribution is planned to take place in the first quarter of 2021. On top of the discussions with its national member groups and user groups, there is ongoing dialogue with industry specific workgroups. The topics for discussion touch upon various domains: revision of standards, service changes, new technology implementations, security enhancements.

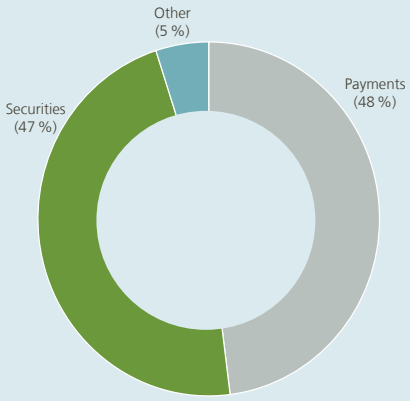
The following two charts give an overview of the 2019 SWIFT FIN activity per market and region. FIN is SWIFT's core messaging service for exchanging financial messages. There are over 11 000 live users of whom 2 420 represent shareholders. Last year, the lion's share of FIN traffic is distributed between payments (48 %) and securities (47 %) messaging. The Europe, Middle East and Africa (EMEA) region took the largest part (64 %) of the total 2019 FIN traffic flow.

1 The national member group is represented by all SWIFT shareholders within the same country. It excludes subsidiaries and branches of foreign financial institutions or corporates. The national member groups are involved in the consultation of product evolutions and technology developments.

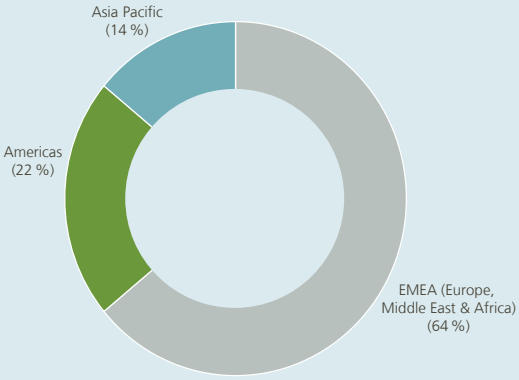
2 The national user groups are made up of SWIFT users from the same country. These groups discuss operational themes (e.g. migrations, standard releases, local trainings, technical implementations affecting users in the country). The national user groups are also involved in the discussions about product developments and technology changes.

SWIFT FIN activity

Breakdown by market



Breakdown by region



International cooperative arrangement

The international cooperative arrangement for the oversight of SWIFT sets out a framework for oversight by the National Bank of Belgium and the central banks of the G10/G20 jurisdictions.

As lead overseer, the NBB conducts the day-to-day follow-up of SWIFT activities and coordinates the different working groups:

The **Cooperative Oversight Group** (OG) consists of the G10 central banks (i.e. Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System, represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System) and the chairperson of the CPMI. The OG discusses oversight policy and strategy. Two OG meetings take place every year.

The **Executive Group** (EG) is a sub-group where direct talks with SWIFT's Board and Executive Management are held on the central banks' oversight policy, issues of concern, SWIFT's strategy regarding oversight objectives, and conclusions. The EG represents the OG in discussions with SWIFT and can pass on OG recommendations to SWIFT. The EG members are Bank of Japan, Federal Reserve Board, Bank of England, European Central Bank and National Bank of Belgium, and meet three times a year.

The G10 **Technical Group** (TG) does the technical fieldwork on important developments within SWIFT and reports back to the OG. Since the TG performs deeper technical analysis, there are four meetings planned each year. At every TG meeting, there is a direct interaction with SWIFT management, internal audit and independent risk functions in order to carry out the technical groundwork for oversight. Skills and

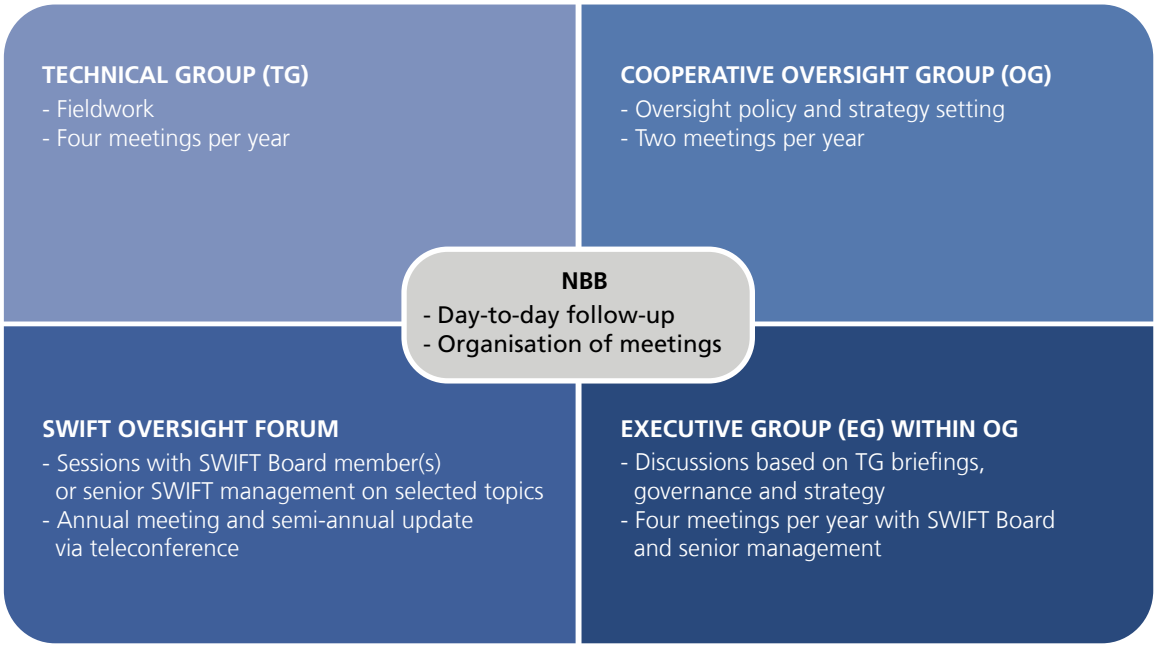
knowledge on technological and IT-specific domains are necessary to better understand these developments and their accompanying risks within SWIFT.

The **SWIFT Oversight Forum** (SOF) involves a larger group of countries, who represent a significant part of the SWIFT traffic volume. This working group consists of the G10 central banks (OG) and 15 additional central banks (i.e. Central Bank of the Argentine Republic, Reserve Bank of Australia, Banco Central do Brazil, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Indonesia, Bank of Korea, Bank of Mexico, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank, Banco de España and Central Bank of the Republic of Turkey). Their membership is aligned with the composition of the CPMI. In 2019, five additional central banks joined the SOF: Central Bank of the Argentine Republic, Banco Central do Brazil, Bank of Indonesia, Bank of Mexico and Banca de España. The SOF holds discussions on oversight policy, provides input for OG priorities, and serves as a platform for communication on system interdependencies related to the common use of SWIFT. The NBB is continuously seeking ways of improving its outreach to other central banks, as indicated in box 12.

The chart below gives an overview of the different working groups involved in the SWIFT oversight.

Chart 6

Cooperative oversight of SWIFT



BOX 12

Outreach activities

In 2018, the IMF recommended the Bank to further extend its information-sharing efforts, which resulted in a series of outreach activities.

The NBB organised its second outreach session at SWIFT's yearly Sibos conference in 2019 in London. More than 70 participants from over 50 countries joined this second session. The advantages of organising the outreach session at SIBOS are threefold: (i) a large delegation of central banks attend the conference, (ii) each time the conference is located in a different continent, (iii) central bank representatives and directors of the payments, IT and FMI oversight departments predominantly attend Sibos.

Oversight expectations

Overseers' core expectations are rooted in five high-level expectations (HLEs): (i) Risk Identification and Management, (ii) Information Security, (iii) Reliability and Resilience, (iv) Technology Planning, and (v) Communication with users[1].

The five HLEs focus on the adequate management of operational and technology risks. SWIFT oversight is structured around the HLEs for its risk-based activities planning, discussions and decisions to take. The five expectations evolved into generic oversight requirements for all critical service providers to FMIs and are formalised in Annex F of the CPMI-IOSCO Principles for FMIs. Overseers expect SWIFT to report back on its compliance with the HLEs. This reporting serves as input for oversight analysis and provides an overview of the risk drivers for SWIFT. As such, enterprise risk management, information security and technology risk management are part of the standing oversight activities covered by the HLEs.

A multitude of approaches with varying intensity and duration are at the overseers' disposal. Box 13 discusses the oversight tools that complement overseers' recurrent analyses on the effectiveness of SWIFT's implementation of the five HLEs.

1 For more detailed information, see FMI Report 2017 or CPMI-IOSCO Principles for FMIs – Annex F: Oversight expectations applicable to critical service providers.

BOX 13

Tools for the oversight of SWIFT

Every TG meeting includes a full day where overseers have a direct interaction with SWIFT management, and second and third lines of defence. SWIFT is invited to update the overseers on developments, incidents, risk reviews, technological changes and projects impacting the entire SWIFT stature.

Senior SWIFT representatives are frequently invited to present their views and directions at OG and SOF meetings. And representatives of SWIFT's Board and Executive Committee attend EG meetings to discuss a variety of topics.

The TG meetings at SWIFT are a snapshot of what is going on in the company and provide overseers with rich information for their work. However, certain developments and changes that are of considerable importance require continuous oversight (e.g. endpoint incident analysis and audit reviews). On top of the four regular TG meetings, ad-hoc meetings with TG members are held whenever necessary to discuss certain topics.

In addition to the technical meeting with SWIFT, overseers have also initiated another oversight tool to gain a better grasp of certain topics and their operations. The already existing interactions with SWIFT give an opportunity to gain broader knowledge. To gain more profound knowledge, deep-dive sessions have been launched. These sessions are designed to gain detailed insight into certain areas, departments, functions, interactions at SWIFT and include the three lines of defence. The deep-dive sessions are arranged at a TG meeting on top of the traditional full-day meeting at SWIFT. Overseers' decision to hold a deep-dive session depends on the consensus reflecting any lack of clear understanding of a certain domain. For example, overseers invite the project owner to explain a major project and its implications on the entire company. So far, overseers have held two deep-dive sessions to obtain deeper knowledge in certain areas.

Another oversight tool that overseers apply at their discretion is the on-site review. The first on-site review kicked off at the end of 2018 and was finalised in 2019. In light of the HLEs, overseers scope a certain area they wish to distinguish so as to look into more closely. Whereas the deep-dive session consists of a half-day discussion on a certain topic, the on-site review is a more dedicated way of understanding a domain and its functioning. Over an entire week, meetings between overseers and different SWIFT representatives are planned. Findings and recommendations are passed on to SWIFT. Accordingly, a follow-up plan is established for which SWIFT is expected to comply with overseers' expectations. Overseers select on-site review topics that are not traditionally fully covered by previous TG oversight tools. An illustration of the objective of the first on-site review was to get a transparent end-to-end overview of the enterprise risk management process.

The SWIFT Customer Security Programme and related fraud detection and prevention tools received considerable attention from overseers in 2019. Also, projects like the ISO20022 migration for cross-border payments traffic have come under overseers' review.

4.2 Covered oversight topics in 2019

Overseers' activities are mainly concentrated around cyber and technological topics. They seek to obtain assurance that the corresponding risks in these domains are adequately assessed, monitored and mitigated in spite of the reliability of the services. Topics like the Customer Security Programme, decisions impacting the IT infrastructure and standing interactions with the three lines of defence were included in the 2019 oversight work.

Customer security programme (CSP)

SWIFT's Customer Security Programme (CSP) aims to strengthen the security of the global financial community against cyber threats by providing requirements for users in terms of how they should secure their own local IT infrastructure used for connecting to SWIFT. In 2019, overseers devoted a considerable amount of time to reviewing the effectiveness of the CSP.

The Customer Security Control Framework (CSCF) has been analysed by overseers on the effectiveness of the implementation and reporting processes. The CSCF is a set of mandatory and advisory controls applicable to every SWIFT user. Mandatory security controls establish a security baseline with which all SWIFT users must comply, whereas advisory controls describe good practices for securing local IT infrastructures. All SWIFT users were required to self-assess their compliance with the CSCF and upload this information through SWIFT's KYC-Self Assessment (KYC-SA) tool by the end of 2019. Overseers observed an uptake in the number of self-attestations in 2019; by 31 December 2019, 91 % of customers, representing 99 % of SWIFT's payments traffic, had attested their level of compliance with the mandatory security controls. Overseers actively follow up on the CSP quality assurance metrics provided by SWIFT. These metrics give an overview of the attestation, consultation, reporting processes' effectiveness, and the security advances across different user types. Quality assurance metrics are continuously being refined and extended by the overseers to improve their monitoring activities.

SWIFT performs an annual review of the CSCF, which overseers review in turn. Other stakeholders are involved in the review process as well, like cyber security experts, supervisory authorities and SWIFT users. Aligned with best practices, two advisory controls were promoted to mandatory and two new advisory controls were added to the most recently updated CSCF version. Multiple existing controls received clarifications on their implementation.

The implementation design of the enhanced KYC-SA supervisory role has been under examination, too. In 2019, the overseers also considered which information supervisors need to perform their activities effectively. SWIFT reserves the right to report users who have failed to timely self-attest full compliance with all mandatory CSCF controls or who depend on non-compliant service providers (i.e. service bureau or shared infrastructure provider) to the competent supervisory authorities. The self-attestation information could be an important input for risk-based planning and scoping for supervisory authorities. Previously, supervisors received information on self-attestation status of BICs in their jurisdiction via SWIFT Post (information push). SWIFT plans to overhaul this process by implementing a supervisory role in the self-attestation tool (information pull).

Overseers reviewed SWIFT's independent assessment framework and will continue to follow-up on the framework's effectiveness over the course of 2020. As of mid-2021, all SWIFT users are required to substantiate their self-attestations with an independent assessment conducted by internal or external auditors. The assessments must cover all applicable mandatory controls specified in the latest version of the CSCF.

Users have the possibility to consult information in their counterparties' CSCF self-attestations to obtain insight into their security position and take appropriate risk-mitigation measures. There has been an increase in counterparty consultations by a varied group of SWIFT users. Overseers will continue to monitor this consultation process. SWIFT's getting started guide for assessing cyber security counterparty risk has also been assessed by overseers.

In 2019, overseers assessed the design and implementation of the recently introduced Payment Control Service (PCS), and existing fraud prevention and detection tools. In addition to the security specifications SWIFT users must comply with, the CSP also sets out how a user can prevent and detect fraud in commercial relationships. SWIFT offers various tools to prevent and detect fraud incidents. The PCS is an example of such a tool. It is an optional tool that aims to help SWIFT users combat fraudulent payments and strengthen their existing security measures.

SWIFT's communication channels to inform its users on technology changes, to interact with compromised users in crisis situations, and to update users on fraud practices of adversaries have been analysed by overseers on their effectiveness and rigour. The CSP also includes how information-sharing in the wider community helps a user to adequately organise incident and risk management processes from any future cyber threats. SWIFT's Information Sharing and Analysis Centre (ISAC) portal contains a large and digestible amount of information targeted to both technical and business professionals on new cyber threats, indicators of compromise, tools and techniques used by hackers.

It is in overseers' interest to obtain reasonable assurance on the effectiveness of the evolving security requirements for users to reduce the risks for SWIFT, its users and the entire community. An important oversight objective is to ensure that these security requirements continue to evolve in line with emerging threats, advances in cyber security practices and regulatory developments.

Other topics

Besides the review of the CSP in the context of financial stability for the wider ecosystem, the core focus remains on the security and availability of SWIFT's critical messaging services.

Cyber security is a top priority for the overseers. Over the course of 2019, overseers continued to focus on the design, implementation and testing of cyber-event detection, response and recovery measures. SWIFT's roadmap setting out its cyber security strategy, improvements and plans has been evaluated and assessed against the strong-changing threat landscape. Furthermore, the impact of new technologies and processes on SWIFT's risk profile have also been closely followed up by overseers. Additionally, overseers have been paying attention to other types of risk than technical ones (e.g. business, third-party risks), namely the recurrent assessment of extreme risks and recovery plans.

Overseers conduct frequent reviews of the effectiveness of the various lines of defence and governance structures for daily operations, long-term strategies and specific projects. In 2019, they challenged these internal and external actors on their opinions, findings and further planned control work. In practice, there have been frequent interactions with SWIFT's Chief Auditor, Chief Risk Officer, and one yearly meeting with the external security auditor. The in-depth review of the enterprise risk management framework kicked off in 2018 and was finalised last year. This review gave better insight into the level of design, integration and implementation of the framework. The first in-depth review has been evaluated as successful and will be a recurrent exercise for the oversight of SWIFT.

Overseers also reviewed how SWIFT applied its cyber security requirements to third-party providers of interface products and shared infrastructure providers. Users can opt to connect to SWIFT through a third party instead of installing the interface products on their premises. Overseers closely followed up on the

security strategy that SWIFT applied to ensure all parties that connect to its network were in accordance with SWIFT's security specifications.

Incidents, like disruptions of SWIFT's services, are closely investigated by overseers. The sequence of events, user impact and results of the outcome of the investigations are analysed. Overseers are informed about the incident and the completeness and adequacy of the corresponding action plans. These action plans are frequently followed up in order to prevent recurrence of similar incidents. The incidents are discussed with SWIFT and further research is carried out if required.

SWIFT's long-term strategy and how it is aligned with specific infrastructure investment often comes under discussion between overseers and SWIFT's management and Board. Overseers typically challenge the security and strategic focus of such plans. For example, they reviewed SWIFT's ISO 20022 migration plan and will follow up on its further progress in 2020 and 2021, and implementation in 2022. Also, the design and roll-out plans of the new interface offering Alliance Cloud have been and will be on the agenda for review.

4.3 Oversight priorities in 2020

The planning of oversight activities results from a risk-based analysis, which is rooted in the five HLEs.

Given the evolving cyberthreat landscape, the focus remains on the adequacy of SWIFT's cyber strategy. More specifically, overseers review the multi-year cyber security roadmap update and progress, which aims at protecting SWIFT's infrastructure, networks and operations. The work of the external security auditor is closely analysed and challenged by overseers.

Overseers will continue to dedicate their support and devoted attention to the CSP. The importance of maintaining the CSCF control framework and monitoring thereof will remain in overseers' standing focus of activities. Relevant metrics to monitor the effectiveness of the Programme will be maintained. Furthermore, overseers continue to engage the refinement of existing and request of additional metrics. As in previous years, focus will be placed on the level of compliance with the security controls, the continued appropriateness of the mandatory control set in a changing environment, the effectiveness of the adherence promotion mechanisms (i.e. assurance, attestation and reporting processes) and the outreach to the different stakeholders. Special attention will be paid to the proposed enhancements of the self-attestations (i.e. independent assessment framework, counterparty consultation, information pull for supervisory authorities).

These major areas of focus are complemented with continuous monitoring activities structured in line with the HLEs.

First of all and in line with our mission, overseers continuously monitor the effectiveness of the three lines of defence (i.e. SWIFT's management, independent risk management function and internal audit function). More specifically, overseers review the management's risk identification and assessments, as well as the effectiveness of the mitigating measures. The development and implementation of the entire ERM methodology and risk acceptance processes are periodically reviewed by overseers. Furthermore, internal and external audit reports are under continuous analysis where overseers follow up on the audit findings and mitigations actions management undertakes.

Secondly, the initiatives that SWIFT undertakes to improve its business continuity management framework and disaster recovery strategies, with respect to the requirements of the CPMI-IOSCO guidance on cyber resilience, are planned for review. More specifically, the focus will be on how SWIFT recurrently assesses

its extreme cyber risk scenarios and its progress towards the achievement of the two-hour recovery time objective (2h-RTO). Referring to the HLEs for information security and technology planning, overseers expect SWIFT to continuously identify gaps and make improvements for their cyber security strategy. The maturity of SWIFT's cyber practices is also planned for continuous review.

Thirdly, overseers will continue assessing the adequacy of processes for monitoring changes in technology risk for the existing infrastructure in place and the maturity of technology performance, scalability, and security for technology choices considering SWIFT's future infrastructure. Confidentiality, integrity and availability are three conditions that are envisaged during overseers' assessment. Recurring topics of attention are SWIFT's third-party vulnerability management and incident response processes.

Fourthly, the initiatives SWIFT is taking to improve communication processes for informing its users will be examined. These involve keeping clients informed about new interface releases (i.e. interface hardening Alliance 7.4 in 2020), updates on new malicious events (e.g. SWIFT ISAC report on new phishing e-mails), interacting with users in crisis situations (e.g. updating incident response guidelines), and engaging in new major developments (e.g. ISO 20022 migration for cross-border payments).

Finally, the overseers will closely analyse the presented design and follow-up of the implementation of major projects and developments that could have a significant impact on SWIFT's critical services and overall risk stature. Discussions with the involved SWIFT representatives of the three lines of defence and breakdown of the relevant documentations are standing practices herein.

BOX 14

COVID-19 impact on SWIFT and oversight activities

As many other international organisations, SWIFT has had to adapt and react to the impact of the pandemic outbreak. Given SWIFT's presence and activities in every continent, it has been monitoring the situation in a timely manner and in accordance with national and local authorities' measures.

As a critical service provider to the financial sector, SWIFT has focused on keeping its critical infrastructure operational to avoid any interruption of global financial messaging traffic. Despite the physical closure of its offices, business continuity has been ensured by promoting working from home for all employees. SWIFT has continuously assessed its staff organisation so that the key staff at the necessary SWIFT locations have been able to work. SWIFT has also reduced the burden on its customers by taking a series of additional mitigating actions, like the one-year delay of new features of its annual standards release.

Most governments have taken measures to limit the economic damage by launching national lockdowns. The global economic slowdown has resulted in an impact on SWIFT messaging. The effects of these measures could be clearly observed in the first half of 2020 (from January until June). Payments traffic grew by 2.1 %, whereas this growth was 4.9 % during the same period last year. In 2019, payments traffic grew by 5.5 %. Securities and treasury traffic grew compared to the same period last year as result of the volatility in the market. Securities posted a growth of 21.7 %, whereas in 2019 this was 8.3 %. In 2019, total securities traffic grew by 9.1 %. Also, treasury traffic showed a similar trend; posting 25.0 % growth in June 2020 compared to 9.4 % in June 2019. Despite the lower payments traffic together with the higher growth of securities and treasury traffic, overall FIN traffic growth was 12.1 %, which was almost double compared to the first semester of 2019 with a growth of 6.6 %.

Overseers adapted their activities to the crisis situation. However, they continued their critical review on SWIFT in areas such as cyber, Enterprise Risk Management, CSP, Internal Audit topics, with in addition COVID-19 implications on the various topics under review. Traditionally, there are multiple physical meetings with different central banks throughout the year. The governmental restrictions such as closed borders and physical distance demanded a decentralised approach to conduct the planned oversight work. Teleconference meetings replaced the physical meetings as the alternative to ensure that the appropriate analysis on SWIFT could be continued. On top of the standing SWIFT oversight meetings, outreach activities also had to be rearranged in another format. In general, the pandemic has not blurred the oversight priorities and overseers continue to profoundly assess SWIFT's activities from a cyber- and operational-risk-based view.